Demetrius Klitou

Privacy-Invading Technologies and Privacy by Design

Safeguarding Privacy, Liberty and Security in the 21st Century
Series Information

The Information Technology & Law Series was an initiative of ITeR, the national programme for Information Technology and Law, which was a research programme set up by the Dutch government and The Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 ITeR has published all of its research results in its own book series. In 2002 ITeR launched the present internationally orientated and English language Information Technology & Law Series. This well-established series deals with the implications of information technology for legal systems and institutions. Manuscripts and related correspondence can be sent to the Series’ Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Editorial Office

T.M.C. Asser Instituut
P.O. Box 30461
2500 GL The Hague
The Netherlands
Tel.: +31-70-3420300
e-mail: itandlaw@asser.nl

Simone van der Hof, Editor-in-Chief
Center for Law in the Information Society (eLaw), Leiden University,
The Netherlands

Bibi van den Berg
Center for Law in the Information Society (eLaw), Leiden University,
The Netherlands

Eleni Kosta
TILT—Tilburg Institute for Law, Technology and Society, Tilburg University,
The Netherlands

Ben Van Rompuy
T.M.C. Asser Instituut, The Netherlands
iMinds-SMIT, Vrije Universiteit Brussel, Belgium

Ulrich Sieber
Max Planck Institute for Foreign and International Criminal Law
Freiburg
Germany
I find the implications of tomorrow’s information society and the advancement of the latest technologies capable of infringing upon the right to privacy and individual liberty extremely relevant, which led me to write this book on the subject.

The discourse in privacy and technology is a legal and political issue, and is more and more a matter of international relations and human rights law. The interplay between politics, ethics, social issues and technology/technological development is a growing phenomenon. Recent examples of the intersection of (international) politics, law, technology and privacy involve the Passenger Name Record (PNR) dispute between the US and EU, the potential worldwide deployment of body scanners, the clash between the European Parliament and EU Council of Ministers over the US-EU SWIFT agreement,1 and the rift between world leaders and the US Government over recently revealed surveillance activities—just to name a few.

Privacy is a fundamental human right, and deserves just as much attention as any other human right. While there are certainly more grave human rights violations across the globe, particularly in Asia and Africa, here in the West, predominantly in the US and the UK, the threat upon the right to privacy and liberty thereof at the hands of those who control advanced technology is and will remain the story of the early twenty-first century. This is still true, I believe, even in the midst of other highly significant and pressing matters, such as the global fight against terrorism, nuclear proliferation, climate change, environmental disasters and the on-going global economic crisis. Indeed, as technology increasingly advances, in terms of its capabilities in intruding upon privacy, collecting and analysing personal data and conducting mass surveillance, I believe the right to privacy will equally become more and more significant.

It is perhaps during crises, particularly as a result of a major terrorist attack, that governments (and citizens) are more likely inclined to support the further development and deployment of technologies capable of safeguarding security. And, in a

---

1 The Society for Worldwide Interbank Financial Telecommunication (SWIFT) manages a global network for exchanging financial messages necessary for facilitating the execution of payment orders/transactions between financial institutions. The US-EU SWIFT agreement allows for the transfer of SWIFT transaction information from the EU to the US.
post-9/11 world, this has indeed occurred. However, the same technologies are often also capable of seriously intruding upon privacy and other civil liberties.

It is important to note that I am certainly not against technology, nor against any governments using technology for maintaining a secure and productive society. I fully support the use of advanced technology, for example, by democratic governments to hunt for terrorists and prevent a terrorist attack, and I recognize that governments are using surveillance technologies to make us safer. They are doing a good job at it. This book does not serve to scaremonger and nor does it argue for the absolute prohibition of surveillance technologies or any other technology capable of invading privacy (i.e., Privacy-Invading Technologies or PITs). I also would like to mostly avoid the social and moral criticism of the rapid development and deployment of PITs. Without arguing against the deployment of PITs, I think we should instead focus primarily on addressing the legal issues at hand and on proposing practical solutions for ensuring that privacy/liberty is always upheld.

The book, instead, serves to point out both the desirable societal benefits and undesirable privacy threats of the latest (privacy-invading) technologies and to recommend how to prevent those threats. I am a technology enthusiast and a supporter of the vast and continuously growing number of digital services (e.g. Google maps, Twitter, etc.) available now online. These are great services. I also especially recognize the infinite possibilities and benefits of technology for society and its well-being. Indeed, for example, the advancement of ICT can address major global societal challenges and provide benefits in terms of commerce, health, mobility, democratic participation, social inclusion, environment and convenience. I am aware that technologies can help governments to serve citizens. Governments use ICT to enhance public security and personal safety and to save lives, for instance, by providing communication capabilities and vital information to first responders, such as digital maps, driving directions, medical information and images. Governments can also use identification technologies, advanced imaging technologies and technologies capable of mass surveillance for better ensuring public/national security. Technology can help us achieve a utopian society.

However, as technology rapidly advances and becomes ever more pervasive, the way and degree to which privacy and liberty may be violated also advances. The right to privacy is becoming ever more difficult to enforce. This has led some to argue that privacy (at least as we know it) will end in the near future, if we do nothing about it (Garfinkel 2001), or is already on its way to ending (Whitaker 2000; Holtzman 2006; O’Hara and Shadbolt 2008), or even has already ended so get over it, and besides what is the use of doing anything about it. At the Centre for Law in the Information Society (eLaw@Leiden), Bart Schermer more specifically argues that privacy will cease to exist in 20 years (2007, 2010). All the same,

---

there is also the strong disbelief that privacy can be concretely ensured in the near future. For some, therefore, the end of privacy and the right thereof is simply inevitable. Accordingly, technology can be used to create a dystopian society.

For these reasons, now more than ever, I believe it is time to thoroughly tackle the great challenges and threats posed by the latest technologies on the right to privacy and other civil liberties, and to thwart the prediction that privacy will end soon. I, for one, also believe that the immense benefits of technology do not have to come at the undesirable expense of privacy and other liberties. A balanced approach is both desirable and possible.

Using all available means and approaches, we must aim to safeguard both privacy/liberty and security in the twenty-first century. If we fail to do so, then we are indeed not just “sleepwalking into a surveillance society” (to quote the UK’s former Information Commissioner, Richard Thomas) but, are rather entering into a nightmarish, dystopian, Orwellian future—which has already begun.

Spring 2014

Demetrius Klitou

References

## Contents

1 **Introduction** ................................................................. 1
   1.1 Escalating Technological Threats to Privacy .......................... 1
   1.2 Core Theme of the Book ............................................... 3
   1.3 Rationale for the Case Studies Selection ............................ 5
   1.4 Key Questions of Interest .......................................... 7
   1.5 Added Value ........................................................... 8
   1.6 Structure and Overview of Chapters ................................ 9
   References ........................................................................... 10

Part I  Principles of Privacy

2 **Privacy, Liberty and Security** ........................................ 13
   2.1 Introduction ............................................................ 13
   2.2 The Concept of Privacy .............................................. 14
   2.3 Privacy as an International Human Right ............................ 17
   2.4 The Merits of Privacy ............................................... 18
   2.5 The Concept of Liberty .............................................. 19
   2.6 Privacy and Liberty .................................................. 20
   2.7 The Concept of Security ............................................ 21
   2.8 Privacy, Liberty and Security ...................................... 22
   References ........................................................................... 25

3 **Assessing the Adequacy of a Privacy Legal Framework** ........ 27
   3.1 Introduction .................................................................. 28
   3.2 An Adequate Privacy Legal Framework? ............................. 28
   3.3 International Consensus in Principle ................................. 29
   3.4 Purpose and Meaning of Each Principle ............................. 31
       3.4.1 Choice/Consent .................................................... 32
       3.4.2 Access/Participation ........................................... 33
       3.4.3 Notice/Awareness ................................................ 34
       3.4.4 Integrity/Security ................................................ 35
       3.4.5 Enforcement/Redress .......................................... 36
   References ........................................................................... 25
Part II  Technological Threats to Privacy

4  Privacy-Invading Technologies ........................................... 49
   4.1  Introduction ................................................. 49
   4.2  A Definition of PITs ....................................... 50
   4.3  The Growing Deployment and Threat of PITs ............... 50
   4.4  PITs and the Human Body .................................. 51
   4.5  PITs and the Public Space .................................. 53
   4.6  Other PITs that May Pose Serious Threats to Privacy and Liberty ... 58
       4.6.1  Neurotechnology .................................. 60
       4.6.2  Unmanned Aerial Vehicles ....................... 61
       4.6.3  Lexid ........................................... 63
       4.6.4  DNA Analysis ................................ 64
       4.6.5  Automatic License Plate Recognition ............. 68
   References ........................................................................ 68

5  Body Scanners: A Strip Search by Other Means? ...................... 71
   5.1  Introduction .................................................. 72
   5.2  A Strip Search by Other Means? ............................ 72
   5.3  How Backscatter Body Scanners Work ..................... 74
   5.4  Security Benefits and Drawbacks ......................... 75
   5.5  The Plausibility of the Threat Posed by Plastic Guns, Ceramic Knives, and Liquid/Chemical and Plastic Explosives ... 77
   5.6  Alternatives to Backscatter Body Scanners ............... 79
   5.7  Scope of Deployment in the US ............................. 84
   5.8  Laws, Codes, Decisions and Other Legal Instruments of Special Relevance in the US .......................... 86
   5.9  Deficiencies and Dilemmas of the US Legal Framework ...... 91
   5.10 Policy-Relevant Recommendations .......................... 99
        5.10.1  Focus on Manufacturer-Level Regulations/Laws .... 99
        5.10.2  Focus on User-Level Regulations/Laws ............ 102
   5.11 Manufacturer-Level or User-Level Regulation? ............. 104
6 Public Space CCTV Microphones and Loudspeakers:  
The Ears and Mouth of “Big Brother” ........................................ 113

6.1 Introduction .......................................................... 114
6.2 The Privacy-Intrusive Evolution of CCTV Surveillance 
Technology ......................................................................... 114
6.3 The Ears and Mouth of “Big Brother” .............................. 116
6.3.1 The Ears (CCTV Microphones) .................................. 118
6.3.2 The Mouth (CCTV Loudspeakers) .............................. 120
6.4 Scope of Deployment in the UK ................................. 121
6.4.1 CCTV Microphones .............................................. 121
6.4.2 CCTV Loudspeakers ............................................... 122
6.5 Security Gains .......................................................... 125
6.5.1 CCTV Microphones .............................................. 125
6.5.2 CCTV Loudspeakers ............................................... 127
6.6 Alternatives to CCTV Microphones and Loudspeakers .... 128
6.6.1 Alternatives to CCTV Microphones .......................... 128
6.6.2 Alternatives to CCTV Loudspeakers ......................... 129
6.7 Laws, Codes, Decisions and other Legal Instruments 
of Special Relevance in the UK .............................................. 130
6.7.1 CCTV Microphones .............................................. 135
6.7.2 CCTV Loudspeakers ............................................... 136
6.8 Deficiencies and Dilemmas of the UK Legal Framework ...... 137
6.8.1 CCTV Microphones .............................................. 137
6.8.2 CCTV Loudspeakers ............................................... 144
6.9 Policy-Relevant Recommendations .................................. 146
6.9.1 CCTV Microphones .............................................. 147
6.9.2 CCTV Loudspeakers ............................................... 149
6.10 Concluding Remarks ............................................... 154
References ........................................................................ 154

7 Human-Implantable Microchips: Location-Awareness 
and the Dawn of an “Internet of Persons” ............................. 157

7.1 Introduction .......................................................... 158
7.2 RFID/GPS Implants and the Technology Behind Them ..... 160
7.2.1 RFID Implants .................................................... 160
7.2.2 GPS Implants ..................................................... 162
7.3 Location-Awareness and the Dawn of an 
“Internet of Persons” ......................................................... 164
7.3.1 The Capabilities of HIMs ....................................... 164
7.3.2 Location Information ............................................ 168
7.3.3 Social and Privacy Implications ................................. 170
7.3.4 A Means of Control ........................................... 171
7.3.5 An “Internet of Persons”: A Possible Dystopian Future? ......................... 172
7.3.6 Are We Nearly There? ........................................ 178
7.4 Potential Security and Well-Being Benefits .............................. 180
7.5 Security Risks and Drawbacks ...................................... 183
7.6 Scope of Deployment .............................................. 187
7.6.1 Actual Deployment in the US .................................. 187
7.6.2 Potential Deployment ......................................... 190
7.6.3 Actual and Potential International Deployment ..................... 198
7.7 Alternatives to HIMs .............................................. 199
7.8 Laws, Codes, Decisions and Other Legal Instruments of Special Relevance in the US .............................................. 201
7.8.1 Constitutionally Protected Rights ............................ 201
7.8.2 Federal Statutory Laws ........................................ 201
7.8.3 Tort Law ...................................................... 204
7.8.4 Case Law ...................................................... 204
7.8.5 State Statutory Laws ........................................... 206
7.8.6 Administrative Decisions ...................................... 207
7.8.7 Standards, Guidelines and Self-regulations ..................... 208
7.9 Deficiencies and Dilemmas of the US Legal Framework ............... 209
7.10 Policy-Relevant Recommendations .................................... 226
7.10.1 Consent ...................................................... 229
7.10.2 Proportionality ................................................. 231
7.10.3 Purpose Specification ......................................... 232
7.10.4 Use Limitation ................................................. 235
7.10.5 Enforcement, Accountability and Redress ....................... 236
7.10.6 Access and Participation ....................................... 238
7.10.7 Notice and Awareness ......................................... 239
7.10.8 Security ...................................................... 241
7.10.9 Privacy Impact Assessment .................................... 242
7.10.10 Definitions .................................................. 243
7.10.11 Constitutional and Case Law Considerations ................. 244
7.10.12 The International Dimension ................................ 245
7.11 Concluding Remarks ................................................ 246
References ........................................................................ 246

8 New Privacy Threats, Old Legal Approaches:
Conclusions of Part II ..................................................... 251
8.1 The New Threats to Privacy .......................................... 251
8.2 Beyond Privacy and Data Protection ................................ 253
8.3 Deficiencies of the Existing Privacy Legal Frameworks ............... 255
Reference ........................................................................ 256
Part III  New Approach to Protecting Privacy

9  The Value, Role and Challenges of Privacy by Design .................. 259
9.1  Introduction ............................................. 260
9.2  Concept, Theory and Origins of PBD .......................... 260
9.3  PBD Methodology ...................................... 266
9.4  PBD Solutions for: Body Scanners, HIMs, CCTV
     Microphones and Loudspeakers .......................... 268
9.5  PBD Versus PETs ....................................... 270
9.6  PBD in the Current US and UK/EU Legal Frameworks ......... 272
     9.6.1  US Legal Framework .......................... 272
     9.6.2  EU Legal Framework .......................... 273
9.7  Growing Widespread Recognition ........................... 274
9.8  Potentially Growing Application .......................... 278
9.9  A Unique Selling Point and Source of Value Creation ...... 279
9.10 The Growing Lack of Trust ................................ 281
9.11 Potential Criticism ...................................... 282
9.12 Practical Challenges of Implementing PBD .................... 283
9.13 Concluding Remarks ..................................... 285
References .................................................. 286

Part IV  Research Results

10 Conclusions and Policy Implications .............................. 291
10.1 Introduction ............................................. 292
10.2 Keeping Up with the Technology ............................ 292
10.3 PBD: Critical Combination of Technology and Law .......... 293
10.4 Not a Substitute for Law .................................. 299
10.5 Flexibility vs. Specificity ................................ 300
10.6 Radical Changes for Radical Capabilities .................... 301
10.7 Implementation, Enforcement, Monitoring and Evaluation .. 306
10.8 Accountability, Sanctions and Recalls ....................... 307
10.9 Certified Privacy-Friendly ................................ 309
10.10 Designing for Privacy ..................................... 311
10.11 Adequate PBD Solutions .................................. 312
10.12 Avoiding Overregulation .................................. 313
10.13 Furthing Deployment and Innovation ......................... 316
10.14 Safeguarding Privacy, Liberty and Security .................. 318
10.15 Using Privacy-Friendly Alternatives ....................... 320
10.16 Countering Potential Criticism of PBD ..................... 320
10.17 Overcoming Some of the Challenges ....................... 321
10.18 Engaging Relevant Stakeholders ........................... 322
10.19 Not a Panacea: The Limitations and Constraints of PBD ............................... 323
10.20 Final Conclusions ........................................ 328
References .................................................. 329

Appendix A: A3-Report ............................... 331

Appendix B: Summary Table .......................... 333

Index ........................................................ 337
Acronyms

ABC Acceptable Behaviour Contract
ACLU American Civil Liberties Union
ACPO Association of Chief Police Officers
AI Artificial Intelligence
ALPR Automatic License Plate Recognition
AMA American Medical Association
AMDA American Medical Directors Association
ASB Anti-social Behaviour
ASBO Anti-social Behaviour Orders
ATD Automatic Threat Detection
ATM Automatic Teller Machine
ATSA Aviation and Transportation Security Act 2001
BAT Best Available Technique
CALEA Communications Assistance for Law Enforcement Act 1994
CAPPS Computer Assisted Passenger Prescreening System
CCTV Closed-Circuit Television
CIA Central Intelligence Agency
CNN Cable News Network
COPPA Children’s Online Privacy Protection Act
CPNI Customer Proprietary Network Information
CTIA Cellular Telecommunications and Internet Association
CTTL Clandestine Tagging, Tracking, and Locating
DARPA Defense Advanced Research Projects Agency
DHS Department of Homeland Security
DNA Deoxyribonucleic Acid
DNS Domain Name System
DPA Data Protection Act 1998
EC European Commission
ECHR European Convention on Human Rights
ECHR European Court of Human Rights
ECPA Electronic Communications Privacy Act 1986
EDPS European Data Protection Supervisor
EHR Electronic Health Records
EPC Electronic Product Code
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPIC</td>
<td>Electronic Privacy Information Center</td>
</tr>
<tr>
<td>ETD</td>
<td>Explosive Trace Detection</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration</td>
</tr>
<tr>
<td>FEC</td>
<td>Federal Election Commission</td>
</tr>
<tr>
<td>FIP</td>
<td>Fair Information Principle</td>
</tr>
<tr>
<td>FIPPS</td>
<td>Fair Information Practice Principles</td>
</tr>
<tr>
<td>FISA</td>
<td>Foreign Intelligence Surveillance Act</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographic Information Systems</td>
</tr>
<tr>
<td>GLN</td>
<td>Global Location Number</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GWOT</td>
<td>Global War on Terror</td>
</tr>
<tr>
<td>HIM</td>
<td>Human-Implantable Microchip</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Rights Act 1998</td>
</tr>
<tr>
<td>HSS</td>
<td>HyperSonic Sound</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant of Civil and Political Rights</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IED</td>
<td>Improvised Explosive Devices</td>
</tr>
<tr>
<td>IID</td>
<td>Improvised Incendiary Device</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transport Systems</td>
</tr>
<tr>
<td>ISE</td>
<td>Information Sharing Environment</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KHz</td>
<td>Kilohertz</td>
</tr>
<tr>
<td>LBA</td>
<td>Location-Based Advertising</td>
</tr>
<tr>
<td>LBS</td>
<td>Location-Based Service</td>
</tr>
<tr>
<td>LEXID®</td>
<td>Lobster-Eye X-ray Imaging Device</td>
</tr>
<tr>
<td>LF</td>
<td>Low Frequency</td>
</tr>
<tr>
<td>LML</td>
<td>Legal Machine Language</td>
</tr>
<tr>
<td>LNL</td>
<td>Legal Natural Language</td>
</tr>
<tr>
<td>LRAD</td>
<td>Long-Range Acoustic Devices</td>
</tr>
<tr>
<td>LPR</td>
<td>Legal Permanent Resident</td>
</tr>
<tr>
<td>Acronyms</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>LVA</td>
<td>Layered Voice Analysis</td>
</tr>
<tr>
<td>MCD</td>
<td>Mobile Computing Device</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-governmental Organization</td>
</tr>
<tr>
<td>NGR</td>
<td>Next Generation Robot</td>
</tr>
<tr>
<td>NIR</td>
<td>National Identity Register</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NORAD</td>
<td>North American Aerospace Defense Command</td>
</tr>
<tr>
<td>PBD</td>
<td>Privacy by Design</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PET</td>
<td>Privacy-Enhancing Technology</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PIT</td>
<td>Privacy-Invading Technology</td>
</tr>
<tr>
<td>PLD</td>
<td>Personal Locating Device</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Record</td>
</tr>
<tr>
<td>PSCO</td>
<td>Police Support Community Officers</td>
</tr>
<tr>
<td>PUF</td>
<td>Physical Unclonable Function</td>
</tr>
<tr>
<td>P3P</td>
<td>Privacy Preferences Project</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>RTD</td>
<td>Research and Technological Development</td>
</tr>
<tr>
<td>SERS</td>
<td>Surface Enhanced Raman Spectroscopy</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>TATP</td>
<td>Triacetone Triperoxide</td>
</tr>
<tr>
<td>TNT</td>
<td>Trinitrotoluen</td>
</tr>
<tr>
<td>TRE</td>
<td>Tag Read Events</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration</td>
</tr>
<tr>
<td>TSO</td>
<td>Transportation Security Officer</td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UDHR</td>
<td>United Nations Declaration of Human Rights</td>
</tr>
<tr>
<td>UDI</td>
<td>User-Driven Innovation</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>UHID</td>
<td>Universal Healthcare Identifier</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>VIRAT</td>
<td>Video Image Retrieval and Analysis Tool</td>
</tr>
<tr>
<td>VCR</td>
<td>Video Cassette Recorder</td>
</tr>
<tr>
<td>VSD</td>
<td>Value-Sensitive Design</td>
</tr>
<tr>
<td>VSS</td>
<td>Voting System Standards</td>
</tr>
<tr>
<td>WBI</td>
<td>Whole Body Imaging</td>
</tr>
<tr>
<td>WTMD</td>
<td>Walk-Through Metal Detector</td>
</tr>
</tbody>
</table>